How Cisco Delivers Software throughout the Enterprise

Network-based software delivery solution improves flexibility, scalability, and security of desktop software distribution.

Cisco IT Case Study / Application Networking Services (WAS IN BUSINESS APPLICATIONS) / Enterprise Software Delivery: This case study describes Cisco IT's internal deployment of Cisco ACNS Software and a third-party software distribution management tool within the Cisco network, a leading-edge enterprise environment that is one of the largest and most complex in the world. Customers can draw on Cisco IT's real-world experience in this area to help support similar enterprise needs.

> "If you are not managing your content, your content is managing you."
>
> **– David Stafford, Technical Lead, Cisco IT Client Technology & Productivity Solutions**

BACKGROUND

IT organizations in midsize to large enterprises have common concerns—one of the most important being how to distribute content, particularly software, quickly and efficiently. Problems around limited network bandwidth and the availability of IT resources complicate the process. Further, without automated replication and delivery of these files, IT operations face additional time and resource demands.

Today, if an enterprise has an automated distribution system at all, it usually consists of Windows-based file servers that store content replicas at various locations. Securing, managing, and maintaining these servers consumes significant IT staff time and increases operating expenses. Equally important, these servers tend to be vulnerable to the same incursions that affect Windows-based desktops.

According to industry consultants, it can take a company as much as 40 IT hours to prepare an application for distribution and to replicate it to users. This assumes standard practices such as conflict tests and quality assurance—but not user acceptance testing, which can take another week or more.

CHALLENGE

The constant need to deliver application updates, security patches, and hot fixes to 50,000 workstations around the globe prompted Cisco® IT in 2002 to look at developing a more efficient, reliable, and cost-effective method of distribution. At the time, Cisco Systems® was averaging 60 to 75 percent penetration for a typical distribution. Desktop management staff were spending valuable time researching which 25 to 40 percent of client devices did not receive a distribution—and why. Table 1 lists the typical types of software distributed throughout Cisco.

Table 1. Typical Types of Software Distributed at Cisco

	Security Updates	Software Application Packages	Configuration Policies	Hard Disk / Partition Images
Average size	20 KB to 5 MB	5 to 500 MB per application	1 to 300 KB	500 MB to 2 GB
Characteristics	Small update files critical to protecting enterprise system stability and security	Greatly varies; often, compiled binaries with limited opportunity for compression	Compressible XML or INI file	Single, compressed, binary file, typically of workstation OS (Windows or Linux)
Relevant software distribution management products	NAI, McAfee VirusScan, Symantec Norton Antivirus, Windows updates	Microsoft Windows Installer, InstallShield, Microsoft SMS, Marimba, Tivoli, Altiris Notification Server	Altiris Agent policy, Network Associates ePolicy Orchestrator	Altiris Deployment Server, Symantec Ghost, PowerQuest Drive Image
File count	Less than 100	1 to 1000 files per application, based on packaging tools and methodology	1 per management system	1 to 5 per enterprise (based on hardware and OS diversity)
Rate of change	Daily to weekly	Weekly	Monthly	Quarterly
Location	Local to client systems at the branches	Core standard is local to client system at the branches; with sufficient bandwidth, software may be remote	Centralized	Local to client system at the branches

One liability of software distribution methods that were in use at Cisco was the inability to assign top priority to important files, such as emergency security patches. “We needed a way to make sure that the network would not be significantly slowed by saturated links back to headquarters when we had an urgent need to protect against the latest incursion.” says Robert Rimmar, manager of the Cisco IT Client Technology & Productivity Solutions team. “We also wanted to end the practice of overnighting CDs to locations that were otherwise unable to get important software updates in a timely fashion.”

Another liability was the lack of a content presence solution. Essentially, Cisco’s legacy system had no way to direct workstations to the closest content source, because client devices did not have the necessary intelligence. Instead, every workstation across the enterprise pointed back to corporate headquarters in search of software updates and patches, a costly process that consumed precious bandwidth with redundant data.

In considering the right approach to the software distribution problem, the Cisco Client Technology & Productivity Solutions team, which led the Cisco IT effort, categorized its concerns as people, process, or technology.

- People – Cisco IT required six full-time employees to manage the nearly 300 Windows servers involved in software distribution. This arrangement created significant production and administrative overhead and assigned too many person-hours to low-value administrative tasks.
- Process – The team wanted to develop a distribution process that would make it unnecessary to manually manage servers and replication of software to them.
- Technology – The team wanted to ensure that users obtained software updates, patches, and antivirus protection from the most efficient network topology possible. Team members knew that their client base was making expensive, inefficient distribution choices, particularly around network traffic and charges to telecommunications providers. They also wanted to avoid the site failure problems that could occur when users attempted to retrieve a patch that a Windows server had been unable to replicate.

Cisco IT set about developing best practices for software distribution. “Our goal was to make software available in a matter of minutes after receiving an update,” says David Stafford, Technical Lead, Cisco IT Client Technology & Productivity Solutions. “We wanted to place software to be distributed in a single area—where it could be easily located. We wanted to be able to abandon the practice of writing custom tools that queried each server to ensure that content had arrived. And we definitely wanted to put an end to complaints when one of our locations discovered that they had not received content.”

SOLUTION

During 2002 and 2003, Cisco IT developed a compelling business case for upgrading its distribution systems for video, application acceleration through caching of HTTP static content, and HTTP worm and virus blocking. The team also had a solution in mind: Cisco Application and Content Networking System (ACNS) Software, a network-based approach that integrated these previously disparate functions. Distributing software via the system was a natural extension of its capabilities.

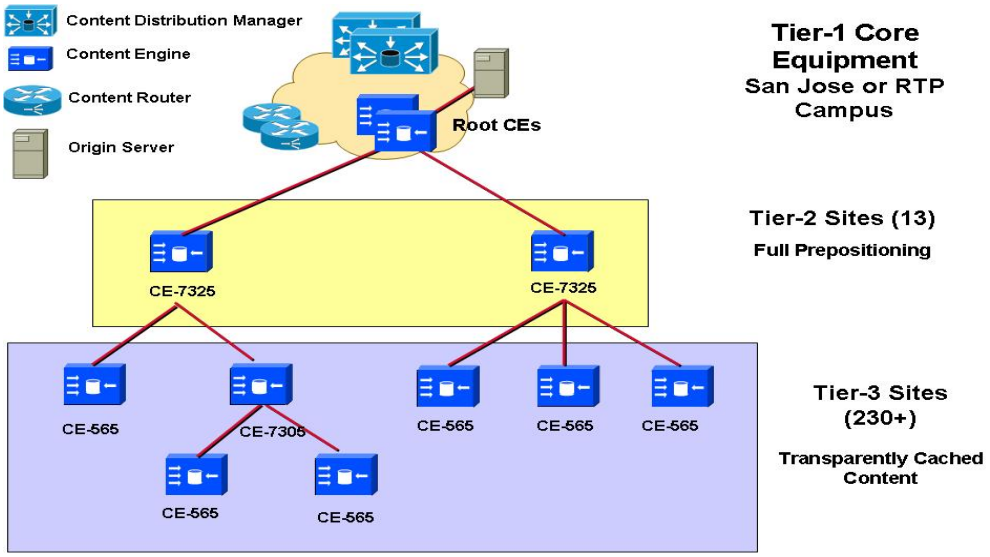
The Cisco ACNS is a one-to-many distribution system for software as well as other forms of content. In graphical terms, this delivery solution looks rather like a pyramid, with a content origin server at the top and an increasingly wider base of appliances (content engines) to which software is disseminated as the viewer moves down the pyramid.

The Cisco ACNS improves IT’s ability to deploy and deliver software by intelligently pre-positioning files near the network edge, close to end-user desktops and product endpoints. The solution allows IT to control WAN bandwidth usage, prioritize software updates, monitor delivery status, and report errors. Handling software images and update files as simply another form of content, the Cisco ACNS also lowers the total cost of ownership (TCO) of software distribution by reducing capital and operating expenses.

Three-Tier Architecture

The Cisco ACNS addresses three crucial elements of content delivery—storage, replication, and presence—through a three-tiered architecture that combines demand-pull caching and pre-positioning to distribute software without overburdening Cisco’s WAN (Figure 1).

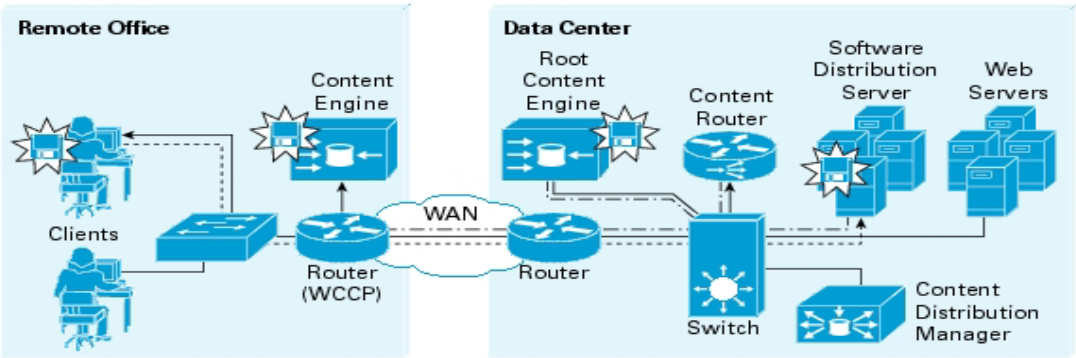
Figure 1. Cisco ACNS Software Solution Three-Tiered Architecture



The Cisco ACNS consists of content engine appliances or network modules for Cisco 2600, 3600, and 3700 Series routers deployed in branch offices or hub locations, and a central content distribution manager that manages the entire system. The content engines are multifunction, plug-and-play devices that eliminate the operating and administrative costs associated with dedicated file servers or network-attached storage (NAS). “One of the best things about content engines,” says Sheila Silveira, manager of the software distribution project, “is that by deploying them at regional hubs or branches, we can offload software distribution processing from multiple central servers, dramatically decrease the consumption of WAN bandwidth during content delivery, get updates out fast—and do it all cost-effectively.” The Cisco Content Distribution Manager’s web-based GUI or Extensible Markup Language (XML)-based API allows administrators to centrally configure, maintain, and monitor content engines, regardless of network location.

Cisco ACNS Software integrates with an off-the-shelf third-party software distribution management agent that automates file replication and scales to accommodate enterprise-class projects. The agent makes it possible for IT to control the distribution process easily through its ability to enforce policies for unicast or multicast distribution, bandwidth management and scheduling, content freshness and availability, and user authentication (Figure 2).

Figure 2. How Cisco ACNS Works with Software Delivery Management Tools



Architecture in Action

The three-tiered Cisco ACNS architecture enables content to be pushed from a central origin server to root content engines, which replicate it to the 13 Tier 2 hub sites. High priority content, such as security or antivirus updates, is also pushed to more than 230 Tier 3 content engines deployed at remote sales and engineering sites.

Business groups within Cisco identify software that should be made available to all employees. The Cisco Content Distribution Manager then categorizes the packages to facilitate the application of different distribution policies and pushes it from the origin server to content engines at Tier 2 hub sites. When users at the local sites request content, the local content engine intercepts the request. If the content has already been pushed to the local site, the local engine serves it from the disk. If not, it requests content from the Tier 2 hub. The net effect is transparent, appearing to the client and client-side software as a native web server. Table 2 lists content functions by tier.

Table 2. Content Functions by Tier

Tier	Function	Location	Content Caching	Content Distribution	Streaming Media	HTTP Worm/Virus Filtering
1	Management, routing, content acquisition	San Jose, California, with backup in Research Triangle Park, North Carolina		X		
2	Content distribution and serving	13 major sites		X	X	
3	Edge caching and limited pre-positioning	Other Cisco offices	X	X	X	X

RESULTS

Using the Cisco ACNS for software distribution and implementing best practices around this use delivered strong business benefits.

Dynamic Scalability

The Cisco ACNS has enabled Cisco IT to effectively scale a single Microsoft IIS web server to provide 60,000 bandwidth-constrained software deliveries—protecting the WAN from outages and allowing distribution to resume seamlessly in case of interruption. The Cisco ACNS can deliver source content from a single origin server to 1 or 2000 content engines, using unicast or multicast replication. Unlike other technologies that do not scale well, the Cisco ACNS Web Cache Communications Protocol (WCCP) transparently redirects clients to the most efficient replicated content source on the network. This network intelligence offers superior scalability, making it easier to manage the overall network and to add new users and sites.

Enhanced Security

The Cisco ACNS enhances the protection of intellectual property through faster distribution of patches, hot fixes, and virus updates, potentially saving millions of dollars a year in system downtime. Because content engines are appliances with closed operating systems, software stored on them is less vulnerable to attack than when it is stored on a Windows server that requires patching as frequently as a work station.

Enhanced Software Distribution

Prior to deploying the Cisco ACNS, manual content replication dramatically slowed software distribution—with 50 percent of a full-time employee's time consumed by creating one copy of each software image file or patch. In addition, the distribution process consumed massive amounts of bandwidth. For example, distributing a 300-MB file (such as Microsoft Office 2003) to more than 230 sites would have taken 12 terabytes, slowing the WAN to a crawl. With the Cisco ACNS solution, distributing such a large file requires only 70 gigabytes of bandwidth.

"Central management and transparent replication of content with the Cisco ACNS makes it just as easy to distribute software to 60,000 desktops as to 60," says David Stafford. "What's more, by making software content available at LAN speed, the ACNS solution slashes the time needed to completely reinstall all software on a laptop or desktop PC. Laptop rebuilds at local LAN speed take 90 minutes, compared to eight hours over the WAN."

The Cisco ACNS also supports automatic virus definition file updates. Whenever new viruses appear (and quickly

spread) across the Internet, Cisco Information Security pushes out new virus updates directly, alerting each PC and laptop to download and install the new virus definition files from the local content engine.

Cisco now achieves 98-percent penetration for every software rollout, compared to 60 to 75 percent with the earlier system, and IT staff members have more time to devote to high-priority projects.

Lower TCO

A number of factors combine to lower the Cisco ACNS total cost of ownership. First, Cisco can amortize the cost of acquiring its hardware and software across different functions because of the multiservice capabilities of the content engines. Second, operating expenses—the cost of managing all aspects of the solution—are greatly reduced by the minimal maintenance and management requirements of these appliances. For example, after a user has connected a content engine to a console and made a few simple configuration changes, the Content Distribution Manager pushes all subsequent changes from a central location. Further, once IT deployed the Cisco ACNS to a second site, the team found that adding 100 or 100,000 client devices created no extra administrative burden within the third-party software distribution management tool.

Increased Employee Productivity and Satisfaction

The ability to distribute software from a content engine on the LAN speeds delivery and decreases the possibility of an urgent software distribution clogging the Cisco WAN during business hours. It also protects employees from the effects of malicious code and speeds the deployment of new PCs, helping to ensure that users and sites are operational quickly.

Greater Flexibility

Using the bandwidth control and prioritization features of the Cisco ACNS, Cisco IT can push software updates to branch offices and pre-position them before users know of their existence. This intelligent content caching ability has greatly reduced Cisco's bandwidth costs at the network edge.

Cisco content engines provide a delivery infrastructure that goes beyond associating client devices with a static delivery path, as some software distribution management tools do. A router in a branch office virtually maps a content engine and can redirect a client device request to the closest content engine when a user moves to a new location—without requiring setting changes. This reduces administrative burden and facilitates user mobility.

LESSONS LEARNED

The Cisco IT Client Technology & Productivity Solutions team has developed a set of robust best practices around the lessons learned during initial deployment of the Cisco ACNS for software delivery.

- Create a cross-functional team – This team should represent desktop, server, and network interests. The desktop and server team members focus on issues such as the technology to use for content storage, replication, and presence; whether that technology can support software updates across different applications and protocols; and how client devices can locate the nearest content engine. Other issues include speed of delivery, user mobility, impact on the WAN, content prioritization, and error reporting. The network team members consider the effect of the system on network topology, bandwidth usage, device usage, and whether WCCP can be used on the routers.
- Include other potential stakeholders – Chances of success improve when other stakeholders, including business and network security managers, can address their concerns. Business managers concentrate on cost justification and measurement of results. Security managers are most concerned with how quickly and effectively security upgrades and patches can be disseminated.
- Develop a clear understanding of the technology – The Cisco ACNS solution rests on caching technology that is well understood by web developers but not necessarily by other IT professionals. Ensuring the success of the deployment involves learning a new vocabulary around content privacy, developing the ability to support content

redirection, and understanding specific syntactical differences between Windows and Linux.

- Identify and characterize all content – This process involves categorizing all files by type of content, size, and how frequently they must be updated. Content requiring the most bandwidth offers the greatest potential for cost saving and helps an implementation team create a strong business case for implementing a new distribution solution.
- Define channels – Create channels, or categories of content; this allows different types of content to be effectively pre-positioned. In the case of the Cisco Content Distribution Manager, define channels and policies using either the graphical user interface (GUI) or XML-based API supported by the Content Distribution Manager. Once a channel has been defined, IT can easily subscribe content engines to it.
- Create a coherent process – Software distribution processes should recognize the myriad factors involved in pushing content across an enterprise. These include priority needs as well as file type and size. For example, prior to the deployment of the Cisco ACNS, IT found that jobs piled up in queue or spontaneously canceled because they were being run at intervals that were significantly shorter than the time consumed by the task. After piloting the new system, Cisco discovered that it needed to develop a coherent set of processes based on its capabilities.
- Pilot and test – After identifying the content from which the enterprise derives the greatest benefit, begin slowly with one or two applications packages. Test in a controlled environment as much as possible to prevent network variables from skewing results. Use cache-hit counters to determine whether or not the local content engine is receiving the hits—a practice that helps to determine return on investment.
- Train and communicate – Educate internal support resources about the systems, including content engine names, channels where updates are stored, how clients are directed to the channels, which origin servers are involved, and how to download a file from a content engine to determine that it is current. Make certain that users understand that they are dealing with appliances, rather than specific servers, and that diagnostics can be safely left to the system designers.

NEXT STEPS

The Cisco ACNS is a one-to-many distribution system for software as well as other forms of content. In graphical terms, this delivery solution looks rather like a pyramid, with a content origin server at the top and an increasingly wider base of appliances (content engines) to which software is disseminated as the viewer moves down the pyramid.

With the Cisco ACNS operating smoothly in a one-to-many environment, a new challenge has emerged. Throughout Cisco, there is a growing need to aggregate nonuniform content from many sources such as laptops, desktops, PDAs, and wireless devices, and house that content in a single location.

Mobile users want data on their laptops, for example, to be available anytime, anywhere—regardless of whether they are using a cell phone or a wireless kiosk in an airport. To make this work, Cisco IT must be able to identify information that is unique to a device, make it easy to access, and protect its integrity.

Cisco IT has begun work on a solution that is based on several technologies—including the Cisco Secure Desktop, wide area file services, third-party synchronization software, single-instance store—and designed to reduce user reliance on a single endpoint.

Regardless of the direction of software distribution, the end result should be the same. Cisco IT is firmly convinced a well-designed, efficient content-delivery network gives all enterprises a powerful tool for keeping mission-critical software current, safeguarding networked resources, optimizing WAN performance, best using IT expertise, and supporting employee productivity.

FOR MORE INFORMATION

To read the entire case study or for additional Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT www.cisco.com/go/ciscoit

NOTE

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties, therefore this disclaimer may not apply to you.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**